AD-781 335

COMPLETE CLASSIFICATION OF (24,12) AND (22,11) SELF-DUAL CODES

Vera Pless, et al

Massachusetts Institute of Technology

Prepared for:

Office of Naval Research

June 1974

BIBLIOGRAPHIC DATA SHEET

1. Report No. MAC TM-49

2.

3. Recipient's Accession No. AD 781 335

4. Title and Subtitle

Complete Classification of (24,12) and (22,11) Self-Dual Codes

5. Report Date : Issued June 1974

6.

7. Author(s)

Vera Pless and N. J. A. Sloane

8. Performing Organization Rept. No. MAC TM-49

9. Performing Organization Name and Address

PROJECT MAC; MASSACHUSETTS INSTITUTE OF TECHNOLOGY:
545 Technology Square, Cambridge, Massachusetts 02139

10. Project/Task/Work Unit No.

11. Contract/Grant No.

N00014-70-A-0362-0006

12. Sponsoring Organization Name and Address

Office of Naval Research
Department of the Navy
Information Systems Program
Arlington, Va 22217

13. Type of Report & Period Covered: Interim Scientific Report

14.

15. Supplementary Notes

16. Abstracts

A complete classification is given of all [22,11] and [24,12] self-dual codes. For each code we give the order of its group, the number of codes equivalent to it, and its weight distribution. There is a unique [24,12,6] self-dual code. Several theorems on the enumeration of self-orthogonal codes are used, including formulas for the number of such codes with minimum distance $\geq$ 4, and for the sum of the weight enumerators of all self-dual codes.

17. Key Words and Document Analysis. 17a. Descriptors

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group

18. Availability Statement

Approved for Public Release;
Distribution Unlimited

19. Security Class (This Report) UNCLASSIFIED

20. Security Class (This Page UNCLASSIFIED

21. No. of Pages 49

22. Price 3.25

THIS FORM MAY BE REPRODUCED

COMPLETE CLASSIFICATION OF (24,12) AND (22,11) SELF-DUAL CODES

by

Vera Pless*
Project MAC, MIT, Cambridge, Massachusetts

and

N. J. A. Sloane
Bell Laboratories, Murray Hill, N. J.

* The work of the first author was supported in part by Project MAC, an MIT interdepartmental laboratory sponsored by the Advanced Research Projects Agency, Department of Defense, under Office of Naval Research Contract N00014-70-A-0362-0006.

COMPLETE CLASSIFICATION OF (24,12) AND (22,11) SELF-DUAL CODES

by

Vera Pless*
Project MAC, MIT, Cambridge, Massachusetts

and

N. J. A. Sloane
Bell Laboratories, Murray Hill, N. J.

ABSTRACT

A complete classification is given of all [22, 11] and [24, 12] self-dual codes. For each code we give the order of its group, the number of codes equivalent to it, and its weight distribution. There is a unique [24, 12, 6] self-dual code. Several theorems on the enumeration of self-orthogonal codes are used, including formulas for the number of such codes with minimum distance ≥ 4, and for the sum of the weight enumerators of all self-dual codes.

* The work of the first author was supported in part by Project MAC, an MIT interdepartmental laboratory sponsored by the Advanced Research Projects Agency, Department of Defense, under Office of Naval Research Contract N00014-70-A-0362-0006.

COMPLETE CLASSIFICATION OF (24,12) AND (22,11) SELF-DUAL CODES

by

Vera Pless
Project MAC, MIT, Cambridge, Massachusetts

and

N. J. A. Sloane
Bell Laboratories, Murray Hill, N. J.

1. Introduction

In spite of 25 years of research ([2], [31]), even the codes of only moderate length, up to 50 say, are a long way from being understood. Slepian [38] used Pólya's counting theorem to find the number of inequivalent codes of length n and dimension k. But the enumeration by length, dimension and minimum distance seems much more difficult. Some results on the enumeration of self-dual codes ($C = C^{\perp}$) have been given in [24], [32], [33], [35]; and in [34] Pless has classified and enumerated all self-dual codes of length $n \leq 20$. In the present paper we first give several new general theorems (§3-§6) including a canonical form for self-orthogonal codes generated by codewords of weight 4(Th. 7.5). We then apply these theorems to enumerate all self-dual codes of length 22 and 24 (§7, §8). For each code we give the order of its group, the number of codes equivalent to it, and its weight distribution. These codes provide 22 and 24 dimensional representations over GF(2) of their groups. There is a unique self-dual code of length 24 and minimum distance 6; its group is a maximal subgroup of $\mathcal{M}_{24}$.

The numbers of inequivalent codes are as follows.

Length n	2	4	6	8	10	12	14	16	18	20	22	24
Indecomposable codes	1	0	0	1	0	1	1	2	2	6	8	26
All Codes	1	1	1	2	2	3	4	7	9	16	25	55

If we require that the weights of codewords be divisible by 4, the corresponding numbers are:

Length n	8	16	24
Indecomposable codes	1	1	7
All Codes	1	2	9

The 9 codes of length 24 with weights divisible by 4 were first found by J. H. Conway (unpublished). Niemeier ([29], see also [28]) has found that there are 24 inequivalent even unimodular lattices in dimension 24, of which 9 correspond to these codes.

[34] also classifies $[n, \frac{1}{2}(n-1)]$ self-orthogonal codes ($C \subset C^{\perp}$) for $n = 1,3,\ldots,19$. Although we have not classified the [21, 10] or [23, 11] self-orthogonal codes, Tables I, II would be of considerable help in doing so.

§2. Terms from Coding Theory

For standard coding theory terms see [2], [31]. All codes are binary and linear. An $[n,k,d]$ (or $[n,k]$ for short) code has length n, dimension k, and (minimum) distance exactly d, and is a subspace of F^n, where $F = \{0,1\}$. $|u|$

denotes the weight of u, and $u \cap v = (u_1 v_1, \ldots, u_n v_n)$. $C^{\perp}$ is the dual code to C. A code is self-orthogonal (s.o.) if $C \subset C^{\perp}$, it is self-dual if $C = C^{\perp}$. The deficiency of a s.o. code is $\delta = \frac{1}{2} n-k$. For a self-dual code, n is even, $\delta = 0$, and the weight of every codeword is divisible by 2. It is possible, and interesting, to require that the weight of every codeword be divisible by 4, in which case n must by a multiple of 8 (c.f. Th. 2.5). Note that if the basis vectors of a self orthogonal code have weight divisible by 4, then all the codewords have this property.

Three important self-dual code are:

(i) The [2, 1, 2] code $C_2 = \{00, 11\}$.

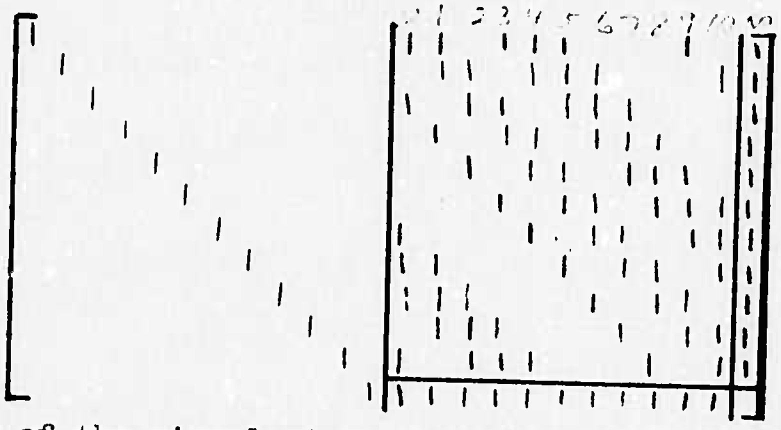
(ii) The [8, 4, 4] Hamming code E_8, which is spanned by the rows of its generator matrix

$$\begin{pmatrix} 1&1&1&1&&&& \\ &&1&1&1&1&& \\ &&&&1&1&1&1 \\ 1&&1&&1&&1& \end{pmatrix} \qquad (2.1)$$

(Blanks denote zeros.)

(iii) The [24, 12, 8] Golay code G_{24}, with generator matrix given by (2.2)([9]).

G_{24}:



(2.2)

(The first row of the circulant on the right of (2.2) has 1's at the quadratic residues modulo 11.)

The (symmetry) group $\mathcal{G}$ (C) of C consists of all permutations of the coordinates which send codewords into codewords (i.e. fix C setwise). $\mathcal{G}$ (C) is a subgroup of the symmetric group $\mathcal{S}_n$. E.g. $\mathcal{G}$ (C_2) is Z_2, the cyclic group of order 2; $\mathcal{G}$ (E_8) is the general affine group $\mathcal{G}\mathcal{A}_3(2)$ of order 1344 (all transformations $\underline{x} \to \underline{x}$ A + $\underline{b}$ where A is an invertible 3×3 matrix); and $\mathcal{G}$ (G_{24}) is the Mathieu group $\mathcal{M}_{24}$ of order $2^{10}.3^3. 5.7. 11.23$ There is an extensive literature on G_{24}, $\mathcal{M}_{24}$, and the associated Steiner system and Leech lattice - see references 1,3,7-10,15,16,19,21, 27,29,33,39,40,42,43.

Two codes C, C′ are equivalent if there exists a permutation in $\mathcal{S}_n$ sending C into C′. The size of the equivalence class continuing C is n! + order of $\mathcal{G}$(C).

The direct sum of codes C[n, k, d] and C′[n′, k′, d′] is the [n+n′, k+k′, min(d,d′)] code $C \oplus C' = \{(u_1 \ldots u_n v_1 \ldots v_n)\colon (u_1 \ldots u_n) \varepsilon C, (v_1 \ldots v_n) \varepsilon C'\}$. $C \oplus C$ will be written 2C, etc. If D can be written $C \oplus C'$ it is called decomposable, otherwise indecomposable ([38]).

If $\mathcal{G}$, $\mathcal{H}$ are groups we write $\mathcal{G} \times \mathcal{H}$ for their direct product, $\mathcal{G}^k$ for $\mathcal{G}\times \ldots \times\mathcal{G}$(k factors), and $\mathcal{G}.\mathcal{H}$ for a semidirect product.

Lemma 2.3 If $C = C_1 \oplus \ldots \oplus C_k$ where the C_i are indecomposable and equivalent then $\mathcal{G}(C) = \mathcal{G}(C_1)^k.\mathcal{S}_k$

Lemma 2.4 Let $C = D_1 \oplus \ldots \oplus D_\ell$ where each D_i is a direct sum of equivalent codes, and for $i \neq j$ no summand of D_i is equivalent to a summand of D_j. Then

$$\mathcal{G}(C) = \prod_{i=1}^{\ell} \mathcal{G}(D_i).$$

Let us say that a self-orthogonal code has property $P(d,\delta)$ if it has minimum distance $\geq d$ and all weights are divisible by δ. Then it is worth mentioning that the number of indecomposable codes with property $P(d,\delta)$ and the total number of all such codes are related by exactly the same Riddell-Gilbert formula ([6], [11], [12], [36 p. 147]) which relates the numbers of connected graphs and all graphs.

The weight distribution of C consists of the numbers $\alpha_0,\ldots,\alpha_n$ where α_i is the number of codewords of weight i. The weight enumerator of C is the polynomial

$\omega(C) = \omega(C;\ x) = \sum_{i=0}^{n} \alpha_i x^i$. E.g. $\omega(C_2) = 1 + x^2$, $\omega(E_8) = 1 + 14x^4 + x^8$, $\omega(G_{24}) = 1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24}$.

Theorem 2.5 (Gleason [13]; see also [4], [14], [23], [25]) (a) The weight enumerator of a self dual code is a polynomial in $\omega(C_2)$ and $\omega(E_8)$. (b) If in addition the weight of every codeword is multiple of 4, then the weight enumerator is a polynomial in $\omega(E_8)$ and ω (G_{24}).

Notation Usually capital Latin letters $(A_{24},\ldots)$ denote codes, the subscript giving the length. d_n, e_n are special codes, & $\underline{1}$, a, a′, b, c are special vectors (see §6). y_{22} and y_{24} are special integers. Capital script letters ($\mathcal{M}_{24}, \ldots$) denote groups.

§3 General Enumeration Theorems

Define, for $0 \leq k \leq \frac{1}{2} n$,

$\Phi_{n,k}$ = the class of self-orthogonal [n,k] codes,

$\Phi'_{n,k}$ = subclass of $\Phi_{n,k}$ of codes which contain $\underline{1}$,

$\Psi_{n,k}$ = subclass of $\Phi_{n,k}$ of codes in which every codeword has weight divisible by 4,

$\Psi'_{n,k}$ = subclass of $\Psi_{n,k}$ of codes which contain $\underline{1}$.

Then $\Phi_{n,\frac{1}{2}n} = \Phi'_{n,\frac{1}{2}n}$ is the class of self dual codes of length n. The following results are useful for enumerating self dual codes. Some of these results appeared in [24], [32], [33]. They are all proved by the methods of [24], [32], i.e. by induction on k. An empty product is equal to 1.

Theorem 3.1 Let n be even and $C \varepsilon \Phi'_{n,s}$. The number of codes in $\Phi'_{n,k} (k \geq s)$ which contain C is

$$\prod_{j=0}^{k-s-1} \frac{2^{n-2s-2j} - 1}{2^{j+1} - 1} .$$

Cor. 3.2 [24] Let n be even and $C \varepsilon \Phi'_{n,s}$. The number of codes in $\Phi'_{n,\frac{1}{2}n}$ which contain C is

$$\prod_{j=1}^{\frac{1}{2}n-s} (2^j+1).$$

Cor. 3.3 [32] The total number of codes in $\Phi'_{n,\frac{1}{2}n}$ is

$$\prod_{j=1}^{\frac{1}{2}n-1} (2^j+1)$$

Cor. 3.4 The total number of codes in $\Phi'_{n,k}$ is

$$\prod_{j=1}^{k-1} \frac{2^{n-2j}-1}{2^j-1} \text{ if n even,} \qquad 0 \text{ if n odd.}$$

Theorem 3.5 Let $C \varepsilon \Phi_{n,s} - \Phi'_{n,s}$. The number of codes in $\Phi_{n,k} - \Phi'_{n,k}$ $(k \geq s)$ which contain C is

$$2^{k-s} \prod_{j=1}^{k-s} \frac{2^{n-2s-2j}-1}{2^j-1} \text{ (n even),} \quad \prod_{j=1}^{k-s} \frac{2^{n-2s-2j+1}-1}{2^j-1} \text{ (n odd).}$$

Cor. 3.6 The total number of codes in $\Phi_{n,k} - \Phi'_{n,k}$ is

$$2^k \prod_{j=1}^{k} \frac{2^{n-2j}-1}{2^j-1} \text{ (n even),} \quad \prod_{j=1}^{k} \frac{2^{n-2j+1}-1}{2^j-1} \text{ (n odd).}$$

Cor. 3.7 Let n be even and $C \varepsilon \Phi_{n,s} - \Phi'_{n,s}$. The number of codes in $\Phi_{n,k}$ $(k > s)$ which contain C is

$$(2^{n-k-s}-1) \prod_{j=1}^{k-s-1} (2^{n-2s-2j}-1) \Big/ \prod_{j=1}^{k-s} (2^j-1).$$

Cor. 3.8 [32] If n is even, the total number of codes in $\Phi_{n,k}$ is

$$(2^{n-k}-1)\prod_{j=1}^{k-1}(2^{n-2j}-1)\Big/\prod_{j=1}^{k}(2^{j}-1).$$

For codes with weights divisible by 4 we do not give as much detail.

Theorem 3.9 Let n be a multiple of 8, and $C\varepsilon\Psi'_{n,s}$. The number of codes in $\Phi'_{n,k} - \Psi'_{n,k}$ $(k > s)$ which contain C is

$$(2^{n-s-k}-2^{\frac{1}{2}n-k})\prod_{j=1}^{k-s-1}\frac{2^{n-2s-2j}-1}{2^{j}-1}$$

Cor. 3.10 Same hypothesis as Th. 3.9. Then the number of codes in $\Psi'_{n,k}$ $(k > s)$ which contain C is

$$(2^{\frac{1}{2}n-s}-1)(2^{\frac{1}{2}n-k}+1)\prod_{j=1}^{k-s-1}(2^{n-2s-2j}-1)\Big/\prod_{j=1}^{k-s}(2^{j}-1)$$

Cor.3.11 [24] Same hypothesis as Th. 3.9. The number of codes in $\Psi'_{n,\frac{1}{2}n}$ which contain C is

$$\prod_{j=0}^{\frac{1}{2}n-s-1}(2^{j}+1).$$

Cor. 3.12 [24] If n is a multiple of 8, the total number of codes in $\Psi'_{n,\frac{1}{2}n}$ is

$$\prod_{j=0}^{\frac{1}{2}n-2}(2^{j}+1).$$

§4. The Sum of all Weight Enumerators

Let

$$\sigma_n(x) = \sum_{C\varepsilon\Phi_{n,\frac{1}{2}n}} \omega(C) \text{ and } \tau_n(x) = \sum_{C\varepsilon\Psi_{n,\frac{1}{2}n}} \omega(C),$$

giving the sum of the weight enumerators of all self dual codes of length n, and the corresponding sum when the weights are divisible by 4.

Theorem 4.1 (a) For n even,

$$\sigma_n(x) = \prod_{j=1}^{\frac{n}{2}-2} (2^j+1)\cdot\left[2^{\frac{1}{2}n-1}(1+x^n) + \sum_{2|i} \binom{n}{i} x^i\right]$$

$$\tau_n(x) = \prod_{j=0}^{\frac{n}{2}-3} (2^j+1)\cdot\left[2^{\frac{1}{2}n-2}(1+x^n) + \sum_{4|i} \binom{n}{i} x^i\right]$$

Proof (a). Write

$$\sigma_n(x) = \sum_{C\varepsilon\Phi_{n,\frac{1}{2}n}} \sum_{u\varepsilon C} x^{|u|}$$

and use Cors. 3.2, 3.3. Similarly (b) follows from Cors. 3.11, 3.12.

Examples

$$\sigma_8(x) = 15(9+28x^2+70x^4+28x^6+9x^8),$$

$$\tau_8(x) = 30(1+14x^4+x^8),$$

$$\sigma_{24}(x) = \frac{305,836,524}{1127}\, y_{24}(2049+276x^2+10626x^4+134,596x^6+735,471x^8 +1,961,256x^{10}+2,704,156x^{12}+1,961,256x^{14} +\ldots+x^{24}),$$

$$\tau_{24}(x) = \frac{596,754}{1127}\, y_{24}(1025+10626x^4+735,471x^6+2,704,156x^{12} +735,471x^{16}+\ldots+x^{24}),$$

where

$$y_{24} = 1.3.5.7. \ \ldots\ .21.23 = 316,234,143,225. \qquad (4.2)$$

§5. Codes with Minimum Distance at least 4

Let C be a s.o. code of length n with minimum distance 2.

Lemma 5.1 C is decomposable if $n > 2$.

Proof. Let $u = (u_1,\ldots,u_n) \varepsilon C$ have weight 2. If $v \varepsilon C$, since $u \cdot v = 0$, $|v \cap u| = 0$ or 2. Let $D = \{v \varepsilon C: |v \cap u| = 0\}$. Then $C = D \cup (u+D)$. Let D′ be obtained from D by deleting the two coordinates i for which $u_i = 1$. Then $C = D \oplus C_2$, $C_2 = \{00, 11\}$.

Lemma 5.2 All codewords of weight 2 in C are nonzero on disjoint sets of coordinates.

Theorem 5.3 Let n be even. The number of s.o. [n, n-r] codes with minimum distance ≥ 4 is

$$\sum_{i=0}^{n/2} \frac{(-1)^i n!}{2^i i!(n-2i)!} a(n,r)$$

where

$$a(n,r) = (2^r-1) \prod_{j=1}^{n-r-1} (2^{n-2j}-1) \Big/ \prod_{j=1}^{n-r} (2^j-1).$$

Proof. Let c(n,r,i) be the number of s.o. [n, n-r] codes containing i codewords of weight 2. From Cor. 3.8,

$$\sum_{i=0}^{n/2} c(n,r,i) = a(n,r).$$

From Lemmas 5.1, 5.2,

$$c(n,r,i) = \frac{n!}{2^i i!(n-2i)!} c(n-2i,r,0),$$

therefore

$$\frac{n!}{2^{\frac{1}{2}n}} \sum_{j=0}^{n/2} \frac{2^j}{(2j)!(\frac{1}{2}n-j)!} c(j,r,0) = a(n,r)$$

The coefficients on the left are those of the Hermite polynomial $H_n(-x)$ [20]. The desired result follows from the orthogonality of these polynomials.

§6. Codes With Minimum Distance Exactly 4

For $n = 4,6,8,\ldots$ let d_n be the s.o. $[n, \frac{1}{2}n-1]$ code with generator matrix

$$d_n: \left[\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & & & & & & & & \\
 & & 1 & 1 & 1 & 1 & & & & & & \\
 & & & & & \cdot & \cdot & \cdot & & & & \\
 & & & & & & 1 & 1 & 1 & 1 & & \\
 & & & & & & & & 1 & 1 & 1 & 1
\end{array}\right]$$

d_n may also be obtained from the $[\frac{1}{2}n, \frac{1}{2}n-1]$ code consisting of all vectors of even weight, upon replacing 0 by 00 and 1 by 11. d_n has deficiency 1, weight enumerator $\frac{1}{2}[(1+x^2)^{n/2}+(1-x^2)^{n/2}]$, and dual code

$$d_n^{\perp} = d_n \cup (a+d_n) \cup (b+d_n) \cup (a'+d_n) \qquad (6.1)$$

where

$$a = 101010\ldots10,$$

$$b = 110000\ldots00,$$

$$a' = a + b = 011010\ldots10. \qquad (6.2)$$

The group of d_n is: $\mathcal{G}(d_4) = \mathcal{S}_4$, $\mathcal{G}(d_n) = Z_2^{n/2} \cdot \mathcal{S}_{\frac{1}{2}n}$ if $n > 4$ ([34]).

For $n = 7, 11, 15, \ldots$ let e_n be the s.o. $[n, \frac{1}{2}(n-1)]$ code with generator matrix

$$e_n: \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & \\ & & & & \cdot & \cdot & \cdot & & & & \\ & & & & 1 & 1 & 1 & 1 & & & \\ & & & & & & 1 & 1 & 1 & 1 & \\ 1 & & 1 & & 1 & & 1 & & 1 & & 1 \end{bmatrix}$$

e_n has deficiency $\frac{1}{2}$, weight enumerator $\frac{1}{2}[(1+x^2)^{(n-1)/2} + (1-x^2)^{(n-1)/2}] + 2^{(n-3)/2}x^{(n+1)/2}$, and dual code

$$e_n^{\perp} = e_n \cup (c+e_n), \qquad (6.1)'$$

where $c = \underline{1} = 11\ldots1$. The group is: $\mathcal{G}(e_7) = \mathcal{GL}_3(2) \simeq \mathcal{PSL}_2(7)$, of order 168; $\mathcal{G}(e_n) = \mathcal{Z}_2^{(n-3)/2}.\mathcal{S}_{\frac{1}{2}(n-1)}$ if $n > 7$([34]).

For $n = 8, 12, 16, \ldots$ let E_n be the $[n, \frac{1}{2}n]$ self-dual code $d_n \cup (a+d_n)$, i.e. with generator matrix

$$E_n: \begin{bmatrix} 1 & 1 & 1 & 1 & & & & & & & & \\ & & 1 & 1 & 1 & 1 & & & & & & \\ & & & & \cdot & \cdot & \cdot & & & & & \\ & & & & & & 1 & 1 & 1 & 1 & & \\ & & & & & & & & 1 & 1 & 1 & 1 \\ 1 & & 1 & & 1 & & 1 & & 1 & & 1 & \end{bmatrix}$$

For E_8 see (2.1). The weight enumerator is $\frac{1}{2}[(1+x^2)^{n/2} +(1-x^2)^{n/2}] + 2^{\frac{1}{2}n-1}x^{n/2}$. The group is: $\mathcal{G}(E_8) = \mathcal{GA}_3(2)$, of order 1344; $\mathcal{G}(E_n) = Z_2^{\frac{1}{2}n-1}\cdot\mathfrak{S}_{\frac{1}{2}n}$ if $n > 8$ ([34]).

Note: In [34], E_8, E_{12}, E_{16}, E_{20} were called A_8, B_{12}, E_{16}, J_{20} respectively. From (6.1), (6.1)' and the fact that E_n is self-dual, we have:

Lemma 6.3 Any codeword of $d_n^{\perp}$ is equal to one of 0,a,b, or a' (modulo d_n); any codeword of $e_n^{\perp}$ is equal to 0 or c(modulo e_n); and any codeword of $E_n^{\perp}$ is equal to 0 (modulo E_n).

Cor. 6.4 If C is a s.o. code containing E_n as a subcode, then C is decomposable.

These codes are important because they provide a canonical form for codes generated by codewords of weight 4, given in Th. 6.5. This result is the basis of the classification in [34] and is used again in §§7,8. The result was derived independently by J. H. Conway (unpublished).

Theorem 6.5 An indecomposable, self-orthogonal code C of length n which is generated by codewords of weight 4 is either $d_n(n = 4,6,8,\ldots)$, e_7 or E_8.

Proof: Let I be the subset of the n coordinate indices with the property that there exists at least one vector in C with 1 on an index in I. We say that C is of type H if I can be partitioned into pairs in such a way that every vector in F^n of weight 4 with ones on any 2 of these pairs is in C. If C is of type H, $|I|$ must be even. Note that a code is of type H iffit is a d_n with $n \geq 4$.

Consider any C. If dim $C = 1$, C is equivalent to d_4. If dim $C = 2$, C is equivalent to d_6. If dim $C \geq 3$, C contains a d_6 and hence must contain a d_n of maximal dimension. Denote this subcode by $\overline{C}$. If $C = \overline{C}$, we are finished. So suppose $C \neq \overline{C}$. Then there is a vector v of weight 4 in $C - \overline{C}$. Since v is orthogonal to all vectors in C we have the following four possibilities.

a) v has no coordinate indices in I.

b) v has 2 coordinate indices in a pair of I.

c) v has 3 coordinate indices in I, no two being in a pair of I.

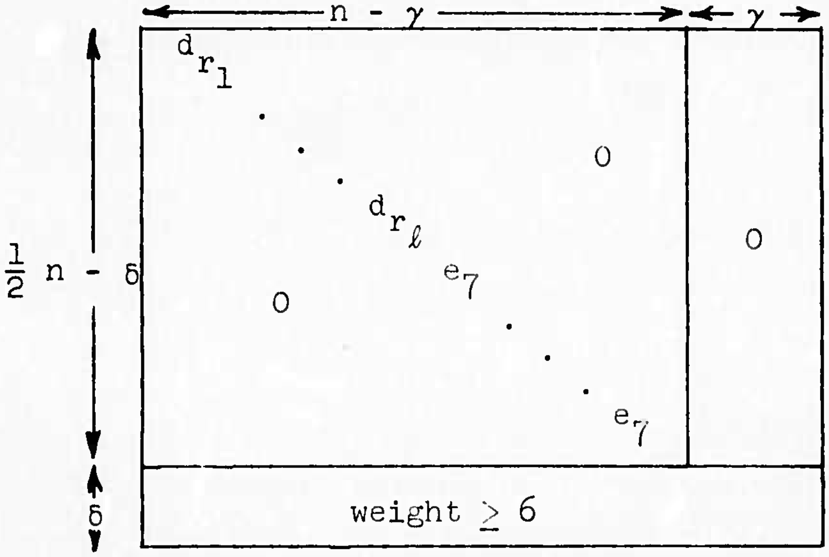
d) v has all 4 coordinate indices in I, no two being in a pair of I.

Since C is indecomposable, case c) implies that $C = e_7$ and case d) implies that $C = E_8$. Case b) is not possible since v could then be added to $\overline{C}$ contradicting its maximal dimension. Case a) is not possible since $\overline{C}$ would then be a direct summand.

<u>Cor. 6.6</u> The only self-dual codes which are generated by codewords of weight 4 are $E_8 \oplus \dots \oplus E_8$.

Our notation for describing the generator matrix of an indecomposable self-dual code C with minimum distance equal to 4 is as follows. We take the maximum number of linearly independent codewords of weight 4 as the top left-hand corner of the generator matrix. By Th. 6.5 and Cor. 6.4

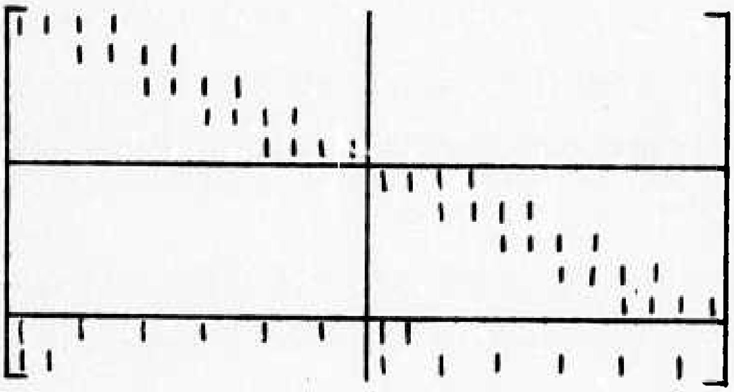
this has the form $d_{r_1} \oplus \ldots \oplus d_{r_\ell} \oplus e_7 \oplus \ldots \oplus e_7$ (with m copies of e_7), or $d_{r_1} \ldots d_{r_\ell} e_7^m$ for short, for suitable $r_1, \ldots, r_\ell, m$. The generator matrix is



It is convenient to use the same symbol (d_r, e_7, etc.) both for the code and its generator matrix. Here γ is called the <u>gap</u> of C, and $\delta = \ell + \frac{1}{2}m + \frac{1}{2}\gamma$ is the deficiency of the subcode generated by codewords of weight 4. The last δ rows have weight ≥ 6. If u is one of the last δ rows, by Lemma 6.3 we may assume that under each d_r, u is one of 0,a,b, or a′ (see(6.2)), and under each e_7, u is either 0 or c.

To avoid writing the generator matrix in full we adopt a shorthand notation, best explained by two examples. The code A_{24} of §8, with generator matrix given in (6.8)

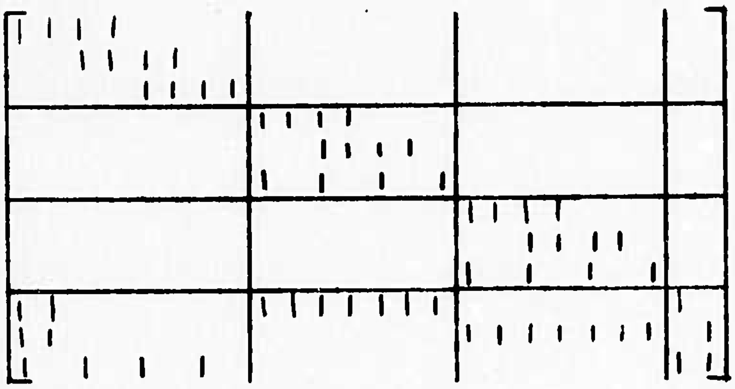
A_{24}:



$$= \begin{bmatrix} d_{12} & 0 \\ 0 & d_{12} \\ a & b \\ b & a \end{bmatrix} \qquad (6.8)$$

will be written $d_{12}^{2}/ab/ba$; and the code J_{24} of §8, with generator matrix given in (6.9)

24:



$$= \begin{bmatrix} d_8 & 0 & 0 & 00 \\ 0 & e_7 & 0 & 00 \\ 0 & 0 & e_7 & 00 \\ b & c & 0 & 10 \\ b & 0 & c & 01 \\ a & 0 & 0 & 11 \end{bmatrix} \qquad (6.9)$$

will be written $d_8e_7^2 + 2/bco10/boc01/ao^21^2$. The explicit form of the generator matrices for indecomposable self-dual codes of length ≤ 20 can be found in [34].

It seems difficult to find a formula for the number of self-dual codes of length n and minimum distance 4. However, the next theorem does provide a useful check on the enumeration of some of these codes.

For $n = 4m$, let Ω_n denote the class of self-dual codes of length n with the property that the codeword $\underline{1}$ is the sum of m disjoint codewords of weight 4. For $C \varepsilon \Omega_n$ let $h(C)$ be the number of ways of writing $\underline{1}$ as a sum of m codewords of weight 4, and let

$$\theta_n = \sum_{C \varepsilon \Omega_n} h(C),$$

$$\varphi_n = \theta_n / \binom{n}{4}\binom{n-4}{4}\cdots\binom{4}{4}.$$

<u>Theorem 6.10</u> An explicit formula for φ_n is

$$\varphi_n = \sum_{i=0}^{m} (-3)^{m-i}\binom{m}{i}\psi_i,$$

where

$$\psi_0 = 1, \quad \psi_i = \prod_{j=1}^{i} (2^j+1).$$

In particular $\varphi_8 = 6$, $\varphi_{24} = 3,811,050$.

Proof By Cor. 3.2, the total number of self-dual codes containing the m codewords

$$\begin{bmatrix} 1111 & & & & \\ & 1111 & & & \\ & & 1111 & & \\ & & & \cdots & \\ & & & & 1111 \end{bmatrix}$$

is $\psi_m = \prod_{j=1}^{m} (2^j+1)$. Each of these codes contains a certain number 2i, where i = 0,1,...,m, of codewords of weight 2. These codewords come in pairs, as each block of 4 coordinates contains 0 or 2 codewords of weight 2. If one of these blocks contains 2 such codewords they can be chosen in 3 ways: 1100 & 0011, 1010 & 0101, or 1001 & 0110. Therefore

$$\psi_m = \sum_{i=0}^{m} 3^i \binom{m}{i} \varphi_{n-4i}, \qquad \text{with } \varphi_0 = 1.$$

Inversion of this recurrence (cf [36,p49]) gives the desired result.

To calculate h(C), it is sufficient to look at the subcode of C generated by codewords of weight 4. It is easily seen that:

$$h(d_n) = \begin{cases} (\tfrac{1}{2}n-1)(\tfrac{1}{2}n-3)\ldots 5.3.1 & \text{if } 4|n \\ 0 & \text{otherwise} \end{cases}$$

$$h(e_7) = 0, \qquad h(E_8) = 7,$$

$$h(d_{r_1} \oplus d_{r_2} \oplus \ldots) = h(d_{r_1})h(d_{r_2})\ldots$$

As an example of Th. 6.10, for $n = 8$ there is one code E_8 in Ω_8, the number of codes equivalent to E_8 is 30 ([34]), and so $\theta_8 = 7.30$, $\varphi_8 = 6$, which agrees with Th. 6.10. For $n = 24$, 15 codes from Table II are in Ω_{24}, namely $3E_8$, $2E_{12}$, $E_8 \oplus E_{16}$, $E_8 \oplus F_{16}$, A_{24}, C_{24}, E_{24}, F_{24}, H_{24}, I_{24}, L_{24}, M_{24}, O_{24}, T_{24} and V_{24}. Again the result agrees with Th. 6.10.

§7. Self Dual Codes of Length 22

Theorem 7.1 There are 25 inequivalent self-dual codes of length 22, 17 of which are decomposable and 8 indecomposable.

These codes are shown in Table I, where for each code C we give:

(i) either its direct sum decomposition if C is decomposable, or a generator matrix in the notation of §6 if C is indecomposable; (ii) the order of the group $\mathcal{G}(C)$; (iii) the number of codes equivalent to C, written as a multiple of

$$y_{22} = 1.3.5.7. \ldots .19.21 = 13,749,310,575;$$

(iv) the weight distribution $\alpha_i = \alpha_{22-i}$ $(i=2,4,\ldots,10)$, omitting $\alpha_0 = \alpha_{22} = 1$.

For codes of length ≤ 20 appearing in Tables I, IJ we use the notation of [34]. Table I also gives the number of codes with minimum distance ≥ 4, and the total number.

These are in agreement with Th. 5.3 and Cor. 3.3. Furthermore the sum of the weight enumerators agrees with Th. 4.1.

Theorem 7.1 is proved by the same method as Theorem 8.1, except that 7.1 is simpler. We omit the details.

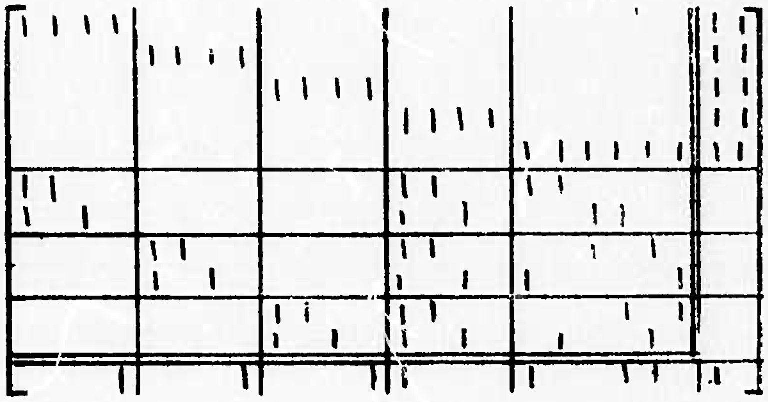
Notes on Table I G_{22} is obtained from the Golay code G_{24} by writing that code as

$$G_{24} = G^{(00)} \cup G^{(01)} \cup G^{(10)} \cup G^{(11)},$$

according to the values of the first two coordinates. Then G_{22} is $G^{(00)} \cup G^{(11)}$ with the first two coordinates deleted. The weight distribution of G_{22} is uniquely determined (given that its minimum distance is 6) from Th. 2.5, or can be obtained from the tables on page 80 of [8]. The group of G_{22} is twice $\mathfrak{M}_{22}$.

U_{22} has generator matrix enclosed by the double line in (7.2).

U_{22} and Z_{24}:



(7.2)

Table I

Self Dual Codes of Length 22

Code	Order of Group	Number ÷ y_{22}	Weight Distribution				
	(I) Decomposable Codes		α_2	α_4	α_6	α_8	α_{10}
$11C_2$	$2^{11}.11!$	1	11	55	165	330	462
$7C_2 \oplus E_8$	$2^7.7!.1344$	$94\frac{2}{7}$	7	35	133	330	518
$5C_2 \oplus E_{12}$	$2^5.5!.2^5.6!$	924	5	25	117	330	546
$4C_2 \oplus D_{14}$	$2^4.4!168^2.2$	$3,771\frac{3}{7}$	4	20	109	330	560
$3C_2 \oplus 2E_8$	$2^3.3!1344^2.2$	$471\frac{3}{7}$	3	31	85	282	622
$3C_2 \oplus E_{16}$	$2^3.3!2^7.8!$	330	3	31	85	282	622
$3C_2 \oplus F_{16}$	$2^3.3!192^2.2$	23,100	3	15	101	330	574
$2C_2 \oplus H_{18}$	$2^2.2!.24^3.6$	123,200	2	10	93	330	588
$2C_2 \oplus I_{18}$	$2^2.2!.168.2^4.5!$	31,680	2	18	85	306	612
$C_2 \oplus E_8 \oplus E_{12}$	$2.1344.2^5.6!$	1,320	1	29	61	258	674
$C_2 \oplus E_{20}$	$2.2^9.10!$	22	1	45	45	210	722
$C_2 \oplus K_{20}$	$2.2^3.4!2^5.6!$	9,240	1	21	69	282	650
$C_2 \oplus L_{20}$	$2.48.168^2$	$30,171\frac{3}{7}$	1	17	73	294	638
$C_2 \oplus S_{20}$	$2.8.192^2$	138,600	1	13	77	306	626
$C_2 \oplus R_{20}$	$2.6.24^3$	492,800	1	9	81	318	614
$C_2 \oplus M_{20}$	$2.4^5.5!$	332,640	1	5	85	330	602
$E_8 \oplus D_{14}$	$1344.168^2.2$	$1,077\frac{27}{49}$	0	28	49	246	700

Table I

Self Dual Codes of Length 22 (cont.)

Code	Generator matrix Order of Group	Number ÷ y_{22}	Weight Distribution				
(II) Indecomposable Codes			α_2	α_4	α_6	α_8	α_{10}
G_{22}	Shortened Golay code $2^8 3^2 5.7.11$	92,160	0	0	77	330	616
N_{22}	$d_{14}e_7+1/bc1/ao1$ $2^6.7!168$	1,508 $\frac{4}{7}$	0	28	49	246	700
P_{22}	$d_{10}^2+2/b^2 1^2/ao01/oa10$ $(2^4.5!)^2.2$	11,088	0	20	57	270	676
Q_{22}	$d_6^2 d_{10}/b^3/a^2 o/a'oa$ $(2^2.3!)^2.2^4.5!.2$	36,960	0	16	61	282	664
R_{22}	$d_6 d_8 e_7+1/boc1/abo1/bao0$ $2^2.3!.2^3.4!.168$	105,600	0	16	61	282	664
S_{22}	$d_6^2 d_8+2/aob10/o^2 a1^2/b^2 o1^2/a^2 o1^2$ $(2^2.3!)^2 2^3.4!.2$	369,600	0	12	65	294	652
T_{22}	$d_4^2 d_6^2+2/aa'bo00/oaao10/aa'ob1^2/oa'oa10/b^2 o^2 1^2$ $4^2.(2^2.3!)^2.2.2$	2,217,600	0	8	69	306	640
U_{22}	$d_4^4+6/\ldots$(see(7.2)) $4^4.4!.6$	2,217,600	0	4	73	318	628

Subtotal with min$^{\underline{m}}$ distance ≥ 4: 5,053,194 $\frac{6}{49}\cdot y_{22}$. Total: 6,241,559 $\frac{34}{49}\cdot y_{22}$.

§8. Self Dual Codes of Length 24

Theorem 8.1 There are 55 inequivalent self dual codes of length 24, 29 of which are decomposable and 26 indecomposable (Table II; for y_{24} see Eq. (4.2)).

Proof. First we find the decomposable codes as direct sums or shorter codes. The groups of these codes are obtained from Lemma 2.4, [34], and Table I. The indecomposable codes are then classified according to minimum distance. By lemma 5.1 there is no indecomposable code with minimum distance 2. It is known [33], [39] that the Golay code G_{24} is the unique code of length 24 and distance 8.

Now suppose the minimum distance is 4. Let C be an indecomposable self dual code of length 24 and distance 4, and let

$$C' = d_{r_1} \oplus \ldots \oplus d_{r_\ell} \oplus e_7 \oplus \ldots \oplus e_7 = d_{r_1} \ldots d_{r_\ell} e_7^m \tag{8.2}$$

be the maximal subcode generated by codewords of weight 4(§6). C′ has gap $\gamma = 24 - r_1 - \ldots - r_\ell - 7m$, and deficiency $\delta = \ell + \frac{1}{2}m + \frac{1}{2}\gamma$.

Our method is to consider each possible form (8.2) for C′, and to find all ways of adding δ linearly independent generators to C′ so as to obtain an indecomposable self dual code C of distance 4. We call such a code C (indecomposable, self dual, minimum distance 4, and with all codewords of weight 4 contained in the subcode C′) an <u>extension</u> of C′. C must

Table II

Self Dual Codes of Length 24 (Page 1)

Code	Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
	(I) Decomposable Codes							
$12\ C_2$	$2^{12}.12!$	1	12	66	220	495	792	924
$8C_2 \oplus E_8$	$2^8.8!.1344$	$141\ \frac{3}{7}$	8	42	168	463	848	1036
$6C_2 \oplus E_{12}$	$2^6.6!.2^5.6!$	1,848	6	30	142	447	876	1092
$5C_2 \oplus D_{14}$	$2^5.5!168^2.2$	$9,051\ \frac{3}{7}$	5	24	129	439	890	1120
$4C_2 \oplus 2E_8$	$2^4.4!1344^2.2$	$1,414\ \frac{2}{7}$	4	34	116	367	904	1244
$4C_2 \oplus E_{16}$	$2^4.4!2^7.8!$	990	4	34	116	367	904	1244
$4C_2 \oplus F_{16}$	$2^4.4!192^2.2$	69,300	4	18	116	431	904	1148
$3C_2 \oplus H_{18}$	$2^3.3!24^3.6$	492,800	3	12	103	423	918	1176
$3C_2 \oplus I_{18}$	$2^3.3!168.2^4.5!$	126,720	3	20	103	391	918	1224
$2C_2 \oplus E_8 \oplus E_{12}$	$2^2.2!.1344.2^5.6!$	7,920	2	30	90	319	932	1348
$2C_2 \oplus E_{20}$	$2^2.2!2^9.10!$	132	2	46	90	255	932	1444
$2C_2 \oplus K_{20}$	$2^2.2!2^3.4!.2^6.6!$	55,440	2	22	90	351	932	1300
$2C_2 \oplus L_{20}$	$2^2.2!48.168^2$	$181,028\ \frac{4}{7}$	2	18	90	367	932	1276
$2C_2 \oplus S_{20}$	$2^2.2!8.192^2$	831,600	2	14	90	383	932	1252
$2C_2 \oplus R_{20}$	$2^2.2!.6.24^3$	2,956,800	2	10	90	399	932	1228
$2C_2 \oplus M_{20}$	$2^2.2!4^5.5!$	1,995,840	2	6	90	415	932	1204
$C_2 \oplus E_8 \oplus D_{14}$	$2.1344.168^2.2$	$12,930\ \frac{30}{49}$	1	28	77	295	946	1400
$C_2 \oplus G_{22}$	$2^9.3^2.5.7.11$	1,105,920	1	0	77	407	946	1232

Table II

Self Dual Codes of Length 24 (Page 2)

Code	Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
	(I) Decomposable Codes							
$C_2 \oplus N_{22}$	$2.2^6.7!.168$	$18,102\frac{6}{7}$	1	28	77	295	946	1400
$C_2 \oplus P_{22}$	$2.(2^4.5!)^2.2$	133,056	1	20	77	327	946	1352
$C_2 \oplus Q_{22}$	$2^2.(2^2.3!)^2 2^4.5!$	443,520	1	16	77	343	946	1328
$C_2 \oplus R_{22}$	$2.2^2.3!2^3.4!168$	1,267,200	1	16	77	343	946	1328
$C_2 \oplus S_{22}$	$2^2.(2^2.3!)^2.2^3.4!$	4,435,200	1	12	77	359	946	1304
$C_2 \oplus T_{22}$	$2^7.(2^2.3!)^2$	26,611,200	1	8	77	375	946	1280
$C_2 \oplus U_{22}$	$2.4^4.4!.6$	26,611,200	1	4	77	391	946	1256
$3E_8$	* $1344^3.3!$	$134\frac{34}{49}$	0	42	0	591	0	2828
$E_8 \oplus E_{16}$	* $1344.2^7.8!$	$282\frac{6}{7}$	0	42	0	591	0	2828
$E_8 \oplus F_{16}$	$1344.192^2.2$	19,800	0	26	64	271	960	1452
$2E_{12}$	$(2^5.6!)^2.2$	1,848	0	30	64	255	960	1476
(II) Indecomposable Codes								
A_{24}	* d_{12}^2/ab/ba(see(6.8)) $(2^5.6!)^2.2$	1,848	0	30	0	639	0	2756
B_{24}	* $d_{10}e_7^2$/bcc/aoc $2^4.5!168^2.2$	$18,102\frac{6}{7}$	0	24	0	663	0	2720
C_{24}	* $d_8^3(a)$/abb/bab/bba $(2^3.4!)^3.3!$	46,200	0	18	0	687	0	2684

Table II

Self Dual Codes of Length 24 (Page 3)

Code		Generator Matrix Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
(II) Indecomposable Codes (Cont.)									
D_{24}	*	$d_6^4(a)$/baao/obaa/aoba/aaob							
		$(2^2.3!)^4 4!$	246,400	0	12	0	711	0	2648
E_{24}	*	d_{24}/a							
		$2^{11}.12$	2	0	66	0	495	0	2972
F_{24}	*	$d_4^6(a)$/boa^3o/$oboa^3$/ $aoboa^2$/a^2oboa/a^3obo/oa^3ob							
		$4^6.5!3$	221,760	0	6	0	735	0	2612
G_{24}	*	Golay code (see (2.2))							
		$2^{10}.3^3.5.7.11.23$	8,013 $\frac{21}{23}$	0	0	0	759	0	2576
H_{24}		d_8d_{16}/ab/ba							
		$2^3.4!2^7.8!$	1,980	0	34	64	239	960	1500
I_{24}		$d_4d_8d_{12}$/b^3/a^2o/oa^2							
		$2.2!2^3.4!2.^5 6!$	110,880	0	22	64	287	960	1428
J_{24}		$d_8e_7^2$+2/bco10/boc01/ $ao^2 1^2$ (see(6.9))							
		$2^3.4!168^2.2$	181,028 $\frac{4}{7}$	0	20	64	295	960	1416

Table II

Self Dual Codes of Length 24 (Page 4)

Code	Generator matrix Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
(II)	Indecomposable Codes (Cont.)							
K_{24}	$d_6d_{10}e_7+1/b^2c1/oao1/abo1$							
	$2^2.3!2^4.5!168$	253,440	0	20	64	295	960	1416
L_{24}	$d_8^3(b)/b^3/a^2o/oa^2$							
	$(2^3.4!)^3.3!$	46,200	0	18	64	303	960	1404
M_{24}	$d_8^3(c)/a^3/ba'o/boa'$							
	$(2^3.4!)^3.2$	138,600	0	18	64	303	960	1404
N_{24}	$d_6^2d_{10}+2/b^311/oa^211/abo01/bao10$							
	$(2^2.3!)^22^4.5!2$	887,040	0	16	64	311	960	1392
O_{24}	$d_4^2d_8^2/ab^2o/boao/oboa/baob$							
	$(2.2!)^2(2^3.4!)^2.2$	1,663,200	0	14	64	319	960	1380
P_{24}	$d_4d_6^2e_7+1/ob^2c1/ab^2o0/oaa'o0/boao1$							
	$2.2!(2^2.3!)^2168.2$	2,534,400	0	14	64	319	960	1380
Q_{24}	$d_6^4(b)/aoao/boa^2/oaoa'/oba'a$							
	$(2^2.3!)^4.8$	739,200	0	12	64	327	960	1368

Table II

Self Dual Codes of Length 24 (Page 5)

Code	Generator matrix Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
(II) Indecomposable Codes (Cont.)								
R_{24}	$d_6^2d_8+4/b^2o1^4/bob1^20^2/o^2a01^20/ao^201^3/oao1^30$							
	$(2^2.3!)^22^3.4!.2$	8,870,400	0	12	64	327	960	1368
S_{24}	$d_4d_6^3+2/abo^21^2/oaob10/aob^20^2/boao01/bo^2a10$							
	$2.2!(2^2.3!)^3.2$	17,740,800	0	10	64	335	960	1356
T_{24}	$d_4^4d_8/babab/ba^2oa/oab^2a'/aoba^2/b^2oaa'$							
	$4^4.2^3.4!.8$	4,989,600	0	10	64	335	960	1356
U_{24}	$d_4^2d_6^2+4/ob^2o1^20^2/oa^2o0^31/obob0^21^2/oaoa010^2/b^2o^21^4/a^2o^21010$							
	$4^2(2^2.3!)^2.4$	53,222,400	0	8	64	343	960	1344
V_{24}	$d_4^6(b)/babo^3/obabo^2/o^2babo/o^3bab/bo^3ba/abo^3b$							
	$4^6.6.8$	9,979,200	0	6	64	351	960	1332

Table II

Self Dual Codes of Length 24 (Page 6)

Code	Generator matrix Order of Group	Number ÷ y_{24}	α_2	α_4	α_6	α_8	α_{10}	α_{12}
(II) Indecomposable Codes (Cont.)								
W_{24}	$d_4^3 d_6+6/\ldots$(see(8.10))							
	$4^3.2^2.3!.3!.2$	106,444,800	0	6	64	351	960	1332
X_{24}	$d_4^4+8/\ldots$(see(8.11))							
	$4^4.4!.2$	159,667,200	0	4	64	359	960	1320
Y_{24}	$d_4^2+16/\ldots$(see(8.9))							
	$2^{11}.3^2$	106,444,800	0	2	64	367	960	1308
Z_{24}	see(8.12)							
	$2^{10}.3^3.5$	14,192,640	0	0	64	375	960	1296

Subtotal with min$^{\underline{m}}$ distance 2: 67,369,356 $\frac{9}{49}\cdot y_{24}$

*Subtotal with weights divisible by 4: 542,744 $\frac{362}{1127}\cdot y_{24}$

Total: 556,041,557 $\frac{86}{1127}\cdot y_{24}$

contain the vector $\underline{1}$. So for each C′ we must find all its extensions C. Lemma 6.3 is our chief weapon. Having found a C, we compute its group $\mathcal{G}(C)$, and then the number of codes equivalent to C is 24!/order of $\mathcal{G}(C)$.

<u>Lemma 8.3</u> $C' = d_{24}$(with $\gamma = 0$, $\delta = 1$) has a unique extension $C = E_{24} = d_{24}/a$ (in the notation of §7).

Proof. We must add 1 vector, u say, to C′. By 6.3 we may assume u is a = 1010...10, b = 1100...00, or a′ = 0110...10. But a′ is equivalent to a, and b has weight 2, so we may take u = a.

The group of E_{24} is $Z_2^{11} \cdot \mathcal{S}_{12}$.

<u>Lemma 8.4</u> $C' = d_r$($4 \leq r \leq 22$) has no extension C.

Proof. By 6.3, the generator matrix of C has the form

$$\begin{array}{r|c|c|} & r & \gamma \\ \hline & d_r & 0 \\ \hline u = & a & \cdots\cdots \\ v = & b & \cdots\cdots \\ \hline & 0 & Q \\ \hline \end{array},$$

where u and v may be absent. If both are absent C is decomposable. If one is absent, Q has deficiency 0, length ≤ 20, and distance 6, which is impossible by Table III. If both u, v are present, Q has deficiency 1. By Table III there <u>is</u> a [20, 9, 6] code Q. But the next lemma shows that this Q, and hence C, does not contain $\underline{1}$, a contradiction.

Table III, which is frequently used in the proof of Th. 8.1, shows, for each dimension k, the length n_0 of the shortest s.o. $[n_0, k, 6]$ code.

Table III

k	1	2	3	4	5	6	7	8	9	10	11	12
n_0	6*	10*	12*	14	15	16*	18	19	20	21	22*	24*

*: code is unique.

This table was constructed by direct search, with the help of [18]. We omit the details. An asterisk indicates that the code is unique. The asterisk for k = 6 follows using the known list of [16, 8, 4] self dual codes [34]. The asterisk for k = 11 is from Th. 7.1.

Lemma 8.5 There is no s.o. [20, 9, 6] code containing $\underline{1}$.

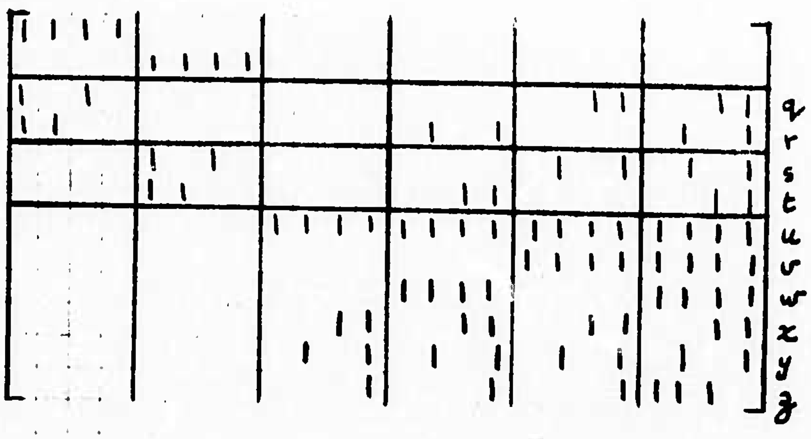
Proof. Suppose such a code D′ exists. By Cor. 3.2 there is a self dual [20, 10, d] code D containing D′. If d = 4, D must be one of the codes E_{20}, K_{20}, L_{20}, M_{20}, R_{20}, S_{20} of [34]. Suppose $D = M_{20}$. Let $v_1, \ldots, v_5$ be the 5 vectors of weight 4 in M_{20}. Then we may assume M_{20} is generated by D′ and v_1. Therefore the following vectors are in D′: $v_1 + v_2$, $v_1 + v_3$, $v_1 + v_4$, hence $v_1 + v_2 + v_3 + v_4 = \underline{1} + v_5$, hence v_5. But v_5 has weight 4, a contradiction. The other possibilities for D, and the case d = 2, are similar.

Lemma 8.6 $d_r d_{24-r}$ (with $\gamma = 0$, $\delta = 2$) has a unique extension $d_r d_{n-r}$/ab/ba provided r = 8, 12. (This gives the entries A_{24}, H_{24} of Table IV).

Lemma 8.7 $d_r d_s$ with $8 < r + s < 24$ has no extension.

Lemma 8.8 d_4^2 has a unique extension $C = Y_{24}$ shown in (8.9).

$Y_{24} =$



(8.9)

Proof. The generator matrix for C must have the form

$$\begin{array}{|c|c|c|l}
\hline
1\,1\,1\,1 & 0 & 0 & \\
0 & 1\,1\,1\,1 & 0 & \\
\hline
a & 0 & \cdots & q \\
b & 0 & \cdots & r \\
\hline
0 & a & \cdots & s \\
0 & b & \cdots & t \\
\hline
0 & 0 & Q & u \\
 & & & \vdots \\
 & & & z \\
\hline
\end{array} ,$$

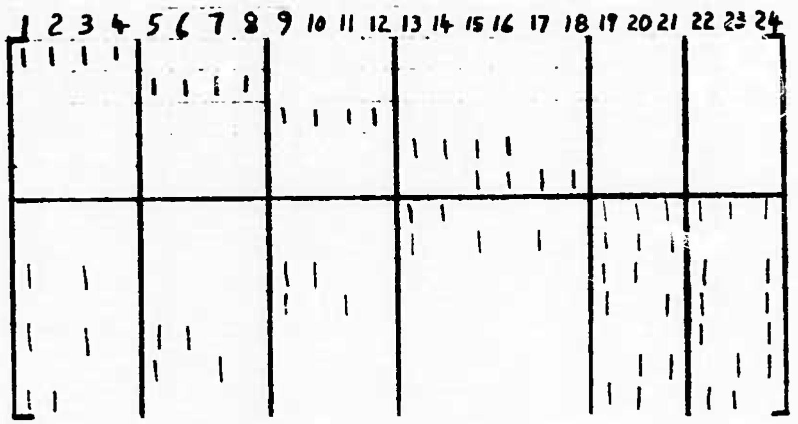
where Q is the unique [16, 6, 6] code mentioned in Table III. To describe Q, let $x_1, \ldots, x_4$ be binary variables. As in describing Reed-Muller codes, we identify each of the 2^{16} polynomials $f(x_1, \ldots, x_4)$ over GF(2) with the corresponding vector of length 16. The first order Reed Muller [16, 5, 8] code R consists of all linear functions $\sum_{i=1}^{4} \alpha_i x_i + \beta$, where α_i, $\beta = 0$ or 1([31]§5.5). Then $Q = R \cup (x_1x_2+x_3x_4+R)$, so we may take as generators for $Q: u=\underline{1}$, $v=x_1$, $w=x_2$, $x=x_3$, $y=x_4$, $z=x_1x_2+x_3x_4$. The group of R is the general affine group $\mathcal{G}a_4(2)$ consisting of all transformations $(x_1,x_2,x_3,x_4) \to (x_1,x_2,x_3,x_4)A + b$, where A is an invertible 4×4 binary matrix and b is a binary 4-tuple.

It is now straightforward to calculate the group of Q, and to show that there is essentially only one way to choose q,r,s,t, namely $q = x_1x_3$, $r = x_2x_4$, $s = x_1x_4$, $t = x_2x_3$, as shown in (8.9).

The group of Y_{24} is as follows. To every permutation π of the first 4 coordinates there corresponds a permutation $g \in \mathcal{G}(Q)$ such that $\pi \circ g$ fixes Y_{24}. Similarly on the second set of 4. Also the two sets of 4 may be exchanged. Finally there are the 16 permutations generated by $x_i \to x_i + 1$ ($i = 1,\ldots,4$). Thus $|\mathcal{G}(Y_{24})| = 24^2.2.2^4$.

The remaining codes in Table II with minimum distance 4 are found in the same way (although none are as complicated as Y_{24}). It is worth pointing out that d_8^3 has three inequivalent extensions: C_{24}, L_{24}, M_{24}; and d_6^4, d_4^6 each have two.

$d_4^3d_6$ has a unique extension W_{24} shown in (8.10),

W_{24}:  (8.10)

and we shall illustrate the general method for finding the group of these codes by calculating $\mathcal{G}(W_{24})$.

The coordinates 1 to 24 of W_{24} are divided naturally into 4 blocks (1 2 3 4)(5 6 7 8)(9 10 11 12)(13 14 15 16 17 18) corresponding to the d_4's and the d_6, plus a gap (19...24). Candidates for $\mathcal{G}(W_{24})$ fall into 3 classes.

(i) For each d_r block, those permutations in $Z_2^{\frac{1}{2}r-1}\cdot\mathcal{S}_r$ which act inside the block, possibly followed by a permutation of the gap (and similarly for each e_7 block, if present). Thus $\mathcal{G}(W_{24})$ contains a Klein 4-group $Z_2\cdot\mathcal{S}_2$ acting on each d_4 block, e.g. (13)(24) and (12)(34) fix the code and generate a Klein 4-group on block 1. Again (13 15)(14 16), (13 17) (14 18), (13 14) (15 16), (13 14) (17 18) generate a $Z_2^2\cdot\mathcal{S}_3$ on block 4.

(ii) Permutations of the blocks, possibly followed by permutations inside the blocks and inside the gap. Thus in W_{24} a group $\mathcal{S}_3$ acts on blocks 1,2,3 as follows. Convention: $\pi\circ\rho$ means first apply π, then ρ. Let π_{12} = (block 1, block 2) = (15)(26)(37) (48), etc. Then

$$\pi_{12}\circ(23)(67)(9\ 11)(19\ 21)(22\ 24)$$

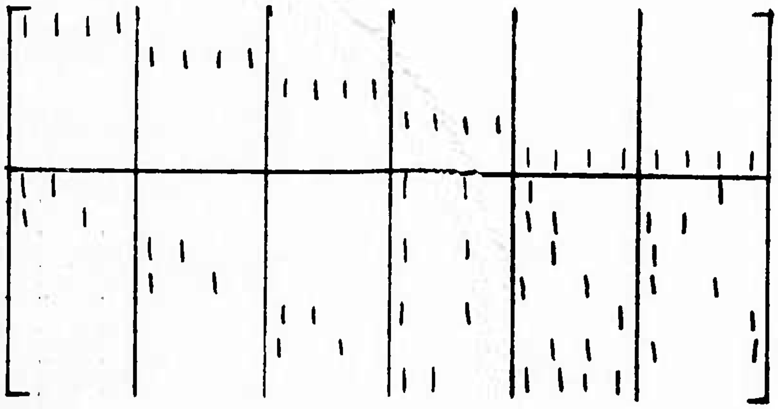
$$\pi_{123}\circ(123)(67)(13\ 14)(19\ 23\ 21\ 22\ 20\ 24)$$

fix the code and generate an $\mathcal{S}_3$ on the blocks.

(iii) Exceptional permutations, not of class (i), which act inside each block, possibly followed by a permutation of the gap. Thus $\mathcal{G}(W_{24})$contains the exceptional permutation (1 2)(5 7)(9 11)(13 14)(19 22)(20 23)(21 24) of order 2. No other permutations of W_{24} are possible, and the order of $\mathcal{G}(W_{24})$ is $4^3.(2^2.3!).3!.2$.

The only codes containing exceptional permutations are F_{24}, W_{24}, X_{24} (8.11) and Y_{24}.

X_{24}:



(8.11)

Finally it remains to consider the case of minimum distance 6. Let C be a [24,12,6] self dual code. By deleting 2 coordinates from C we obtain a [22,11,4] **self** dual code D, which must be in Table I. It is straightforward to show that the only possibility is $D = U_{22}$, and further that there is a unique way to add two columns and one row to the generator matrix of U_{22} to obtain C, as shown in (7.2). Therefore C is unique, and is denoted by Z_{24}.

To simplify calculation of the group of Z_{24}, we give an alternative construction for this code based on the Golay code G_{24}, using the notation of Todd's paper [42].

Let $\Omega = \{\infty,0,1,\ldots,22\}$ be the coordinates of G_{24}. A subset of Ω giving the location of the 1's in a codeword of G_{24} of weight 8 is called an <u>octad</u>. A list of the 759 octads is given in [42]. Ω may be partitioned into 6 sets of 4(called <u>mutually complementary tetrads</u>) such that the union of any two tetrads is an octad, for example (using

Todd's notation for the octads).

∞ 0 1 2, 3 5 14 17, 4 13 16 22, 6 7 19 21, 9 10 15 20, 8 11 12 18.

(*)

Associated with any set of mutually complementary tetrads is a set of 64 <u>non-special</u> <u>hexads</u> (i.e. 6-sets of Ω) with the properties: (i) A non-special hexad is not contained in any octad; and (ii) let $H = (a_1a_2a_3a_4a_5a_6)$ be any non-special hexad, choose any point, say a_1, of H, and find the unique octad $a_2a_3a_4a_5a_6b_2b_3b_4$ containing the other 5 points of H. Then $a_1b_2b_3b_4$ must be one of the tetrads.

A method of constructing the non-special hexads is given in [42]. A set of 12 non-special hexads associated with the tetrads(*) form the rows of (8.12). These rows do indeed generate a [24, 12, 6] code, which therefore must be Z_{24}. The group of this code is that subgroup of $\mathcal{M}_{24}$ which fixes the set of mutually complementary tetrads. This is the group G_5 described in [42], of order $2^{10}.3^3.5$ and index 1771 in $\mathcal{M}_{24}$. The permutations and character table are given in Table VII of [42].

This completes the enumeration of the codes and the proof of Theorem 8.1.

As checks on table II we verified the number of codes of minimum distance ≥ 4 (5.3), the number of codes with weights divisible by 4 (3.12), the sum of the weight enumerators of the latter codes (4.1), the total number of

$$Z_{24}: \quad \left[\begin{array}{cccccccccccccccccccccccc}
\infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 \\
1 &&&& 1 & 1 &&& 1 &&& 1 && 1 &&&&&&&&&& \\
& 1 &&&&& 1 &&&&&& 1 &&&& 1 &&&& 1 &&& 1 \\
&& 1 &&&&& 1 &&& 1 &&&& 1 & 1 &&&& 1 &&&& \\
&&& 1 &&&&&& 1 &&&&&&&& 1 & 1 &&& 1 & 1 & \\
& 1 &&&&&&&& 1 &&&&& 1 & 1 & 1 &&&&&& 1 & \\
&& 1 &&&&&&&& 1 && 1 &&&&& 1 & 1 && 1 &&& \\
& 1 &&&&& 1 & 1 && 1 & 1 &&&&&&& 1 &&&&&& \\
&& 1 &&&&&&&&&& 1 &&& 1 &&&&&& 1 & 1 & 1 \\
& 1 &&& 1 &&&&&& 1 &&& 1 & 1 &&&&&& 1 &&& \\
&& 1 &&& 1 &&&&&&&& 1 && 1 & 1 &&&& 1 &&& \\
&& 1 &&& 1 &&& 1 &&&&&&&&&& 1 & 1 && 1 && \\
&&& 1 && 1 &&&&&& 1 &&&& 1 &&&& 1 &&& 1 &
\end{array}\right] \qquad (8.12)$$

codes (3.3), the sum of all weight enumerators (4.1), and φ_{24} of Th. 6.10.

Cor.8.13 There are 9 self dual codes of length 24 with all weights divisible by 4 (denoted by an asterisk* in Table II).

Cor 8.14 There is a unique self dual code of length 24 and minimum distance 6.

Cor.8.15 Let C be an indecomposable self dual code of length 24, with weight distribution α_i. Either $\alpha_6 = \alpha_{10} = 0$ or $\alpha_6 = 64$, $\alpha_{10} = 960$.

Proof. 1. From Table II; or

2. From Th. 2.5 (using the version in [41]),

the weight enumerator of C is, for suitable ℓ, m,

$$(1+x^2)^{12} - 12x^2(1+x^2)^8(1-x^2)^2 + \ell x^4(1+x^2)^4(1-x^2)^4 + mx^6(1-x^2)^6$$

$$= 1 + (\ell-6)x^4 + (m+64)x^6 + (399-4\ell-6m)x^8 + 15(m+64)x^{10} +\ldots,$$

so $\alpha_{10} = 15\alpha_6$. But the codewords with weights divisible by 4 form a subcode of C of dimension 11 or 12, so $\alpha_6 + \alpha_{10} = 0$ or 2^{10}. This completes the proof.

Remarks (1) The latter proof can be used for lengths 8 and 16 to decide which of the possible weight enumerators given by Th. 2.3 can be realized by codes.

(2) Note that N_{22}, P_{22}, K_{24} can also be written $e_7e_{15}/\ldots, e_{11}^2/\ldots, d_6e_7e_{11}/\ldots$.

Acknowledgements

We thank J. H. Conway for telling us about his enumeration of the self dual codes of length 24 with weights divisible by 4. In the course of this work we have used the ALTRAN ([5],[17]) and MACSYMA ([26],[27]) programs for algebraic manipulation, and R. H. Morris's multiple-precision "desk calculator" on the UNIX System [40]. We also wish to thank Richard Fateman for aid in computations.

REFERENCES

1. E. F. Assmus, Jr., and H. F. Mattson, Jr., Perfect Codes and the Mathieu Groups, Arch. Math. 17 (1966), 121-135.

2. E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, N. Y., 1968.

3. E. R. Berlekamp, Coding Theory and the Mathieu Groups, Info. Control 18 (1971), 40-64.

4. E. R. Berlekamp, F. J. MacWilliams and N. J. A. Sloane, Gleason's Theorem on Self-Dual Codes, IEEE Trans. Info. Theory, 18(1972), 409-414.

5. W. S. Brown, ALTRAN User's Manual, Bell Laboratories, 2nd Ed., Murray Hill, N.J., 1972.

6. C. C. Cadogan, The Möbius Function and Connected Graphs, J. Comb. Theory 11(B) (1971), 193-200.

7. J. H. Conway, A Perfect Group of Order 8, 315, 553, 613, 086, 720, 000 and the Sporadic Simple Groups, Proc. Nat. Acad. Sci. USA, 61 (1968), 398-400.

8. J. H. Conway, A Group of Order 8, 315, 553, 613, 086, 720,000, Bull. London Math. Soc. 1 (1969), 79-88.

9. J. H. Conway, A Characterization of Leech's Lattice, Inventiones Math. 7 (1969), 137-142.

10. J.H. Conway, Three Lectures on Exceptional Groups, Pages 215-247 of "Finite Simple Groups", edited by M. B. Powell and G. Higman, Academic Press, N.Y., 1971

11. G. W. Ford and G. E. Uhlenbeck, Combinatorial Problems in the Theory of Graphs, I, Proc. Nat. Acad. Sci. U.S.A., 42 (1956), 122-128.

12. E. N. Gilbert, Enumeration of Labeled Graphs, Can. J. Math., 8 (1956), 405-411.

13. A. M. Gleason, Weight Polynomials of Self-Dual Codes and the MacWilliams Identities, Actes, Congr. Inter. Math., Nice 1970, Gauthier-Villars, Paris, Vol. 3 (1970), 211-215.

14. J. M. Goethals, F. J. MacWilliams, and C. L. Mallows, Further Remarks on Extremal Self-Dual Codes, to appear.

15. M. J. E. Golay, Notes on Digital Coding, Proc. IEEE 37 (1949), 657.

16. M. J. E. Golay, Binary coding, IEEE Trans. Info. Theory 4 (1954), 23-28.

17. A. D. Hall, Jr., The ALTRAN System for Rational Function Manipulation - A Survey, Commun. Assoc. Computing Machinery, 14 (1971), 517-521.

18. H. J. Helgert and R. D. Stinaff, Minimum-Distance Bounds for Binary Linear Codes, IEEE Trans. Info. Theory, 19(1973), 344-356.

19. M. Karlin, New Binary Coding Results by Circulants, IEEE Trans. Info. Theory 15(1969), 81-92.

20. M. G. Kendall and A. Stuart, The Advanced Theory of Statistics, Vol. 1., Hafner, N.Y., 1969, pp. 155-156.

21. J. Leech, Some sphere packings in higher space, Can. J. Math., 16 (1964), 657-682.

22. J. Leech and N. J. A. Sloane, Sphere Packings and Error-Connecting Codes, Can. J. Math., 23 (1971), 718-745.

23. F. J. MacWilliams, C. L. Mallows, and N. J. A. Sloane, Generalizations of Gleason's Theorem on Weight Enumerators of Self-Dual Codes, IEEE Trans. Info. Theory 18(1972), 794-805.

24. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, Good Self Dual Codes Exist, Discrete Math., 3 (1972), 153-162.

25. C. L. Mallows, and N. J. A. Sloane, An Upper Bound for Self-Dual Codes, Info. Control 22(1973), 188-200.

26. W. A. Martin and R. J. Fateman, The MACSYMA System, Proc. Second A. C. M. Symposium on Symbolic and Algebraic Manipulation, Los Angeles, Calif., March 1971.

27. Mathlab Group, Project MAC, "MACSYMA Reference Manual", MIT Cambridge Mass., version 5, June 1973.

28. J. Milnor and D. Husemoller, Symmetric bilinear forms, Springer-Verlag, Berlin, 1973 (Appendix 4).

29. H.-V. Niemeier, Definite quadratische Formen der Dimension 24 und Diskriminante 1, J. Number Theory 5 (1973), 142-178.

30. L. J. Paige, A Note on the Mathieu Groups, Can J. Math., 9 (1957), 15-18.

31. W. W. Peterson and E. J. Weldon, Jr , Error- Connecting Codes, 2nd Edition, MIT Press, Cambridge, Mass., 1972.

32. Vera Pless, The number of isotropic subspaces in a finite geometry, Accad. Naz. Lincei., Rend. Cl. Sci. Fiz., Mat. e Nat., (8) 39 (1965), 418-421.

33. Vera Pless, On the Uniqueness of the Golay Codes, J. Combin. Theory, 5 (1968), 215-228.

34. Vera Pless, A Classification of Self-Orthogonal Codes over GF(2), Discrete Math., 3 (1972), 209-246.

35. Vera Pless and J. N. Pierce, Self-Dual Codes over GF(q) Satisfy a Modified Varshamov Bound, Information and Control, 23(1973), 35-40.

36. John Riordan, An Introduction to Combinatorial Analysis, Wiley, N. Y., 1958.

37. John Riordan, Combinatorial Identities, Wiley, N.Y., 1968.

38. D. Slepian, Some Further Theory of Group Codes, Bell Syst. Tech. J., 39 (1960), 1219-1252. (Reprinted in "Algebraic Coding Theory: History and Development", I. F. Blake editor, Dowden, Hutchinson and Ross, Stroudsberg, Pennsylvania, 1973.)

39. S. L. Snover, The Uniqueness of the Nordstrom - Robinson and Golay Binary Codes, Ph.D. dissertation, Michigan State University, East Lansing, Mich; August, 1973.

40. R. Stanton, The Mathieu groups, Can. J. Math., 3(1951), 164-174.

41. K. Thompson and D. M. Ritchie, UNIX Programmer's Manual, 2nd Edition, Bell Laboratories, Murray Hill, N.J. 1972.

42. J. A. Todd, A Representation of the Mathieu Group M_{24} as a Collineation Group, Ann. di Math. Pura ed Appl., (IV) 71(1966), 199-238.

43. E. Witt, Über Steinersche Systeme, Abb. Math. Sem. Univ. Hamburg, 12(1938), 265-275.